Adatvédelem és információszabadság

2. ZH jegyzet

Madarász Bence

2017. 05. 11.

A PET technológiák fajtái, csoportosítása

Privacy-enhancing technologies

A PET olyan **információs és kommunikációs technológiák gyűjtőfogalma**, amelyek **megerősítik az egyén magánéletének védelmét** egy információs rendszerben azáltal, hogy **megakadályozzák a személyes adatok szükségtelen vagy jogellenes felhasználását**, vagy olyan eszközöket és beavatkozási lehetőségeket kínálnak, amelyek növelik az egyén ellenőrzését személyes adatai felett.

A PET az információs-kommunikációs technológiai intézkedések olyan rendszere, amely az **információs privacy-t a személyes adatok kezelésének kiiktatásával vagy minimalizálásával védi**, és így megakadályozza a személyes adatok szükségtelen vagy nemkívánatos kezelését, anélkül, hogy csökkentené az információs rendszer funkcionalitását.

Biztonsági technológiák: a főnököt, a szervezetet védik a támadók ellen

PET-ek: a gyengébb felet (az adatalanyt) védik az erősebb féllel szemben

Célja, hogy ne csak az adatokat, hanem az adatok alanyait is védjék a visszaélések ellen és biztosítsák az adatalanyok információs önrendelkezését.

Kritiériumok

- Anonimitás
- Pszeudonimitás
- Megfigyelhetetlenség
- Összeköthetetlenség

PET-ek csoportosítása

- A
  - szubjektum-orientált (anonim kártyabirtokosok)
  - objektum-orientált (anonim digitális pénz)
  - tranzakció-orientált (rekordok automatikus törlése)
  - rendszer-orientált (a fenti elemek egybefűzése)
- B
  - meglévő rendszerek biztonságát növelő technológiák
  - új adattárolási és -hozzáférési technikák
  - tranzakció-alapú technológiák
- C
  - Az alapján, hogy melyik adatvédelmi alapelv érvényesülését segíti elő
- D
  - Technológia alapú PET-ek (hitelesítés azonosítás nélkül)
  - Humán interakció alapú PET-ek
- E
  - egyedi problémák megoldását célzó technológiák (anonim böngésző)
  - rendszerszintű megoldást nyújtó technológiák (PRIME)
  - vizualizáló technikák (email path visualizers)

PET példák

Anonim bögészők, remailerek, cookie írtók, spyware írtók, webpoloska írtók, spamszűrők és adblockerek

Bioszkript

Biometrikus rejtjelezés
Olyan technológia, amely **nem egyetlen felhasználói tevékenységtípus védelmére irányul**. Alkalmazható például a személyazonosító adatok és más **személyes adatok ideiglenes szétválasztására**, ún. „anonim adatbázisok" felépítésére. Használható az elektronikus levelezésben vagy az elektronikus kereskedelmi szolgáltatásokban. **A bioszkript létrehozásához két kiinduló adatra: egy biometrikus és egy nembiometrikus adatra van szükség**. A biometrikus adat lehet egy ujjlenyomat digitális képe, a nembiometrikus pedig egy kriptográfiai kulcs, egy azonosító kód vagy egy mutató (pointer), de akár egy haiku is lehet. **A két adat összekódolásából jön létre a bioszkript**, amelyet a biometrikus adattal, mint afféle kulccsal lehet felnyitni, és így lehet hozzáférni a további alkalmazáshoz szükséges nembiometrikus adathoz. A gyakorlatban a biometrikus adat ismételt produkálása az ujjlenyomat újbóli leolvasását jelenti, s így biztosítható, hogy az alkalmazás az érintett személyek jelenlétében és feltételezett hozzájárulásukkal történjék.

Kapcsolati kód

Szerepe, hogy az adatalanyokat **egyértelműen azonosítsa két adatkezelés közötti kapcsolatban**, ugyanakkor **szegmentálja a személyesadat-köröket**, amelyeket az egyes adatkezelők megismerhetnek. A kapcsolati kód alkalmazását egyébként a nagy állami nyilvántartások közötti adatkapcsolatban törvény is elrendeli Magyarországon, de szervezeten belüli alkalmazásuk is hasznos lehet, például a személyazonosító adatoknak a többi személyes adatról való leválasztására. Az egyik adatállományban például a nevek és az egyedi kapcsolati kódok szerepelhetnek, a másikban csak a kapcsolati kódok és az érdemi adatok - így a túloldalon látszólag anonimizált egyedi **adatsorokhoz juthatunk, amelyek** személyes volta ugyan a kapcsolati kód segítségével bármikor helyreállítható, azonban **személyes mivoltuktól ideiglenesen megfosztott formájukban alkalmasak arra, hogy kezelésük garanciákat nyújtson a személyes adatok jogellenes kezelése ellen.**

Anonim remailer

Olyan üzenettovábbküldő szolgáltatásokról van szó, amelyek akár a címzett elől is elfedik a küldő kilétét. Többnyire azonban a címzett ismeri a feladót, kettejük kapcsolatából csak a harmadik feleket kívánják kizárni.
Alapkövetelmények

- A kommunikáló partnerek anonimitása
- A partnerek közötti kapcsolat nyomonkövethetetlensége
- Az üzenet tartalmának megfejthetetlensége
- A remailer kompromittálhatatlansága

Típusai

- Pszeudonim remailer (csak nevet cserél)
- Cypherpunk (aszimmetrikus titkosítású)
- Mixmaster (többféle kódolás, fix méretű csomagok)
- Mixminion (összetett kulcskezelés, álforgalom)

A remailer szolgáltatás használatakor először le kell kérdezni az éppen aktív remailerek listáját, a felhasználónak választania kell egy programot. Az üzenetküldő lánc már automatikusan alakul ki. Tekintettel az olykor **jelentős** - szándékos - **késleltetés**ekre, **a remailerek nem a sürgős üzenetküldés, hanem a biztonságos és bizalmas kommunikáció eszközei**.

Közadat-hozzáférést támogató rendszerek

A közérdekű adatok központi elektronikus jegyzéke
Közzétételi listák

- általános közzétételi lista
- különös közzétételi listák
- egyedi közzétételi listák

Egységes közadatkereső

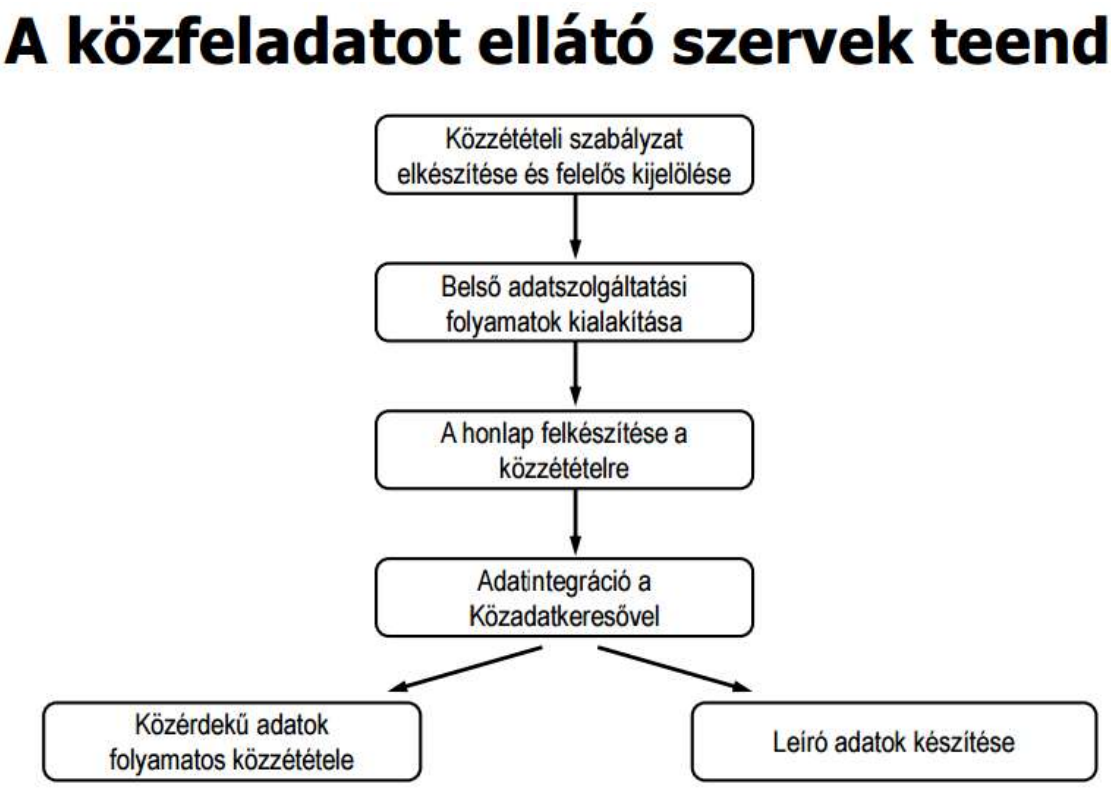
Az elektronikus közzétételre kötelezett **adatgazdáknak regisztrálniuk kell a www.kozadattar.hu weboldalon**, le kell tölteniük az ingyenes szoftvernek a saját rendszerükhöz illeszkedő nyelvű verzióját, majd pedig a közzétett közérdekű adatok és **dokumentumok leíró adatait** (*metaadatait*) – például a dokumentum típusát, keletkezésének időpontját, pontos webcímét – **be kell írniuk egy egyszerű táblázatba, amit aztán az internetre kötött rendszer automatikusan „learat".** A regisztrációs és adatfeltöltési fegyelem serkentésében és ellenőrzésében sem a korábbi adatvédelmi biztosok, sem a jelenlegi hatóság nem jeleskedtek, ezért **a rendszer adattartalma hiányos**. Ezzel együtt nyilvánvalók az előnyei az internetes keresőgépek találataival szemben: amíg az általános keresők találatainak relevanciája, időszerűsége és megbízhatósága kérdéses, addig **a közadatkereső ellenőrizhető adatokat szolgáltat**, az adatgazdák felelősségével.
Open Archives Initiative (OAI)

- webes tartalommegosztás
- interoperábilis adat- és dokumentumtárak létrehozása és működtetése
- metaadat-megosztás
- publikálás
- archiválás
- szabványosítás
- résztvevők:
    - Archive
    - Data Provider
    - Service Provider

Az Átlátszó.hu szolgáltatásai

Az Átlátszó.hu **internetes oknyomozó, tényfeltáró portál** 2012-ben online közérdekűadatigénylő szolgáltatást indított KiMitTud néven. **Az igénylők egy előre elkészített levélsablonba írhatják kérdésük lényegét, kereshetnek az adatgazdák között; a rendszer figyeli a válasz törvényes határidejének leteltét**, válasz híján automatikusan újraküldi az adatigénylést, valamint közzéteszi a feltett kérdéseket és a

válaszokat. 2015 júliusáig mintegy 5.200 adatigénylést kezelt a szolgáltatás és 4.704 adatgazda kapcsolati adatait tette elérhetővé. Az Átlátszó, tizenkilenc további országban működő testvér-szolgáltatásával közösen, az Alaveteli nevű, finn fejlesztésű, ingyenes és nyílt forráskódú, közadatkérést segítő szoftvert használja. Számos előnye mellett a szoftver **kritikájaként említhető, hogy ugyan az, hogy az egyéni adatigénylők mit kérdeznek és arra a hatóságok mit válaszolnak, maga is közérdekű adat, de az, hogy ki kérdezi, az nem** – az Alaveteli rendszer azonban ezt is nyilvánosságra hozza.



A TOR hálózat alapjai

A TOR projekt célja a szabad kommunikáció biztosítása azokban az országokban, ahol a szólásszabadság korlátozott. A **névtelenség biztosításának egyik eszköze** a TOR. A rendszer lehetővé teszi, hogy a felhasználók **anélkül látogassanak meg weboldalakat, hogy azok azonosítani tudnák** akár **a felhasználót**, akár az országot, ahonnan a kérés indult. Mivel a rendszer az egyszer kialakított **adatútvonalakat véletlenszerű időközökben felszámolja és újakat épít** ki, valamint a TOR rendszeren belül **minden kommunikáció titkosítva és fragmentálva kerül továbbításra,** a kommunikáció akkor is bizalmas marad, ha a hálózatba rosszindulatú tag épül be. Az **exitnode** *(ahol a kommunikáció kilép a TOR hálózatból)* **a kommunikáció tartalmát ismeri, a kommunikáció másik résztvevőjét azonban nem**. A TOR rendszerek keresztül elérhető sávszélesség általában jelentősen alacsonyabb, mint a közvetlen internetkapcsolaton mért.

A PRIME architektúra

A **jelenleg futó legjelentősebb PET vonatkozású európai uniós projekt** a 2004-ben indult PRIME (*Privacy and Identity Management for Europe*). A PRIME projektek **végső célja, hogy az információs rendszerekbe egy middleware szerű, alkalmazás- és platform-független réteget építsenek bele**, amely a felszín alatt elvégzi mindazokat a teendőket, amelyeket akár a jogszabályi előírások, akár az adatkezelő önszabályozása, akár az érintett adatalanyok egyéni preferenciái meghatároznak. Ha **például egy adatot az adatkezelési cél teljesülésével törölni kell, a PRIME réteg automatikusan követi az adat sorsát a különböző adatkezelőknél és gondoskodik a törléséről**. Amint a projekt elnevezése is utal rá, **központi eleme az identitásmenedzselés.** E kifejezés alatt általában azt értik használói, hogy miként tudja ügyfeleinek adatait minél jobban menedzselni az üzleti szolgáltató vagy a hatóság. A PRIME ezzel szemben felhasználó-központú identitásmenedzselést kíván megvalósítani, ahol – a jogszabályi korlátok között – **maguk a felhasználók határozhatják meg adataik sorsát**, és annak teljesítéséről automatikus rendszerek gondoskodnak.

A belső adatvédelmi felelős

Az adatvédelmi törvény 2004. január 1-én hatályba lépő – az EU szabályozásnak megfelelő – új rendelkezései szerint **belső adatvédelmi** *(és nem adatbiztonsági)* **felelőst kell kinevezni számos adatkezelőnél, s a törvény a felelősök feladatait is előírja. Adatvédelem: az, amivel a belső adatvédelmi biztosnak kell foglalkoznia 2004. január 1-től.**

Hol	Kötelező-e	Ki lehet
• országos hatósági, munkaügyi vagy bűnügyi adatállományt kezelők • pénzügyi szervezetek • elektronikus hírközlési szolgáltatók • közüzemi szolgáltatók	IGEN	jogi, közigazgatási, informatikai „vagy ezeknek megfelelő, felsőfokú végzettség”
• külön jogszabályban meghatározott szervezetek	IGEN	az ott meghatározott végzettséggel
• egyéb helyen	NEM	bárki

A belső adatvédelmi felelősök konferenciája

- a NAIH elnöke hívja össze
- évente legalább egyszer
- szakmai egyeztetés, egységes gyakorlat kialakítása
- a törvény által előírt BAF-oknak kötelező
- más BAF-oknak opcionális

Nemzetközi adatvédelmi szabályozás

Európai Tanács egyezmény: Egyezményen és EU-n kívüli harmadik országba csak akkor **küldhető korlátozás nélkül személyes adat**, ha az a megkövetelt adatvédelmi szintet megüti *(azonos, ekvivalens védelem)*
EU direktíva: **Megfelelő** *(adekvát)* **védelem** eltérő környezetben, **alternatív eszközökkel** és módszerekkel is elképzelhető.
Egy nem-adekvát védelmi kategóriás országba irányuló személyes információáramlást korlátozni kell, mely problémákat vet fel.
Az adatvédelmi reform a **magánélet védelmét szolgáló eszközöket, illetve a szabályszegő cégek elleni bírságolás lehetőségét is magában foglalja**. A jövőbeli egyeztetéseken szintén központi szerepet kap a felhasználói beleegyezés definíciójának kérdése, valamint az, hogy a cégek milyen feltételekkel használhatják, tárolhatják és használhatják újra egyéb célokra személyes adatokat. Felállna egy, a nemzeti hatóságokból álló **Európai Adatvédelmi Tanács** (EDPB) az elé utalt ügyekben való beavatkozásra.
EU/USA Adatvédelmi pajzs
Korábbi safe harbour fejlesztése: privacy shield. Az EU-USA Adatvédelmi Pajzs egy megfelelési nyilatkozattételre épül, melynek következményeként **az amerikai vállalatok kötelesek megfelelni számos adatvédelmi alapelvnek,** azaz az EU-USA Adatvédelmi Pajzs Keretrendszer Alapelveinek.

- A Tájékoztatási Alapelv
- Az Adatok Sértetlensége és a Célhozkötöttség Alapelve
- A Választás Jogának Alapelve
- Az Adatbiztonság Alapelve
- A Hozzáférhetőség Alapelve
- A Jogorvoslat, Végrehajthatóság és Felelősség Alapelve
- A Másodlagos Továbbításért Való Felelősség Alapelve
- Felügyelet és végrehajtás
- A Pajzs elhagyása